## Chairman Latta—Opening Statement "Do Not Call: Combating Robocalls and Caller ID Spoofing" Subcommittee on Digital Commerce and Consumer Protection April 27, 2018

(As prepared for delivery)

Good morning. We thank our witnesses for being here today. We especially appreciate your patience and flexibility adjusting your travel plans after this hearing was rescheduled from last week.

Thank you for being here to help us explore the range of solutions and strategies available to consumers to combat the scourge of robocalls, caller ID spoofing, and telemarketing scams. It is critical that we help consumers understand their options when it comes to robocalls and spoofing.

For example, consumers can download robocall-blocking apps for their mobile phones, or contact their landline and wireless providers for call-blocking options.

They can register their home or mobile phones with the National Do Not Call Registry, which protects their number from legitimate telemarketing calls they do not want to receive.

And there are common sense strategies like not answering calls from unknown numbers and not following any prompts if you do not know who the call is from—for example do not "press 1 to take your name off this list."

Good options are available, but I think all of us, including industry, can and should do a much better job of education, particularly with our seniors, to make sure that new scam ideas are stopped quickly.

So what's a robocall? When the phone rings with an automated, prerecorded telemarketing message that's a robocall. They're a nuisance, and they're illegal. Yet, every day tens of thousands of American consumers report receiving a robocall.

A staggering 3.2 billion robocalls were placed nationwide in the month of March, according to one source. In Ohio's 419 area code alone, my local area code, nearly 12 million robocalls were placed. For every month in the

past year, robocalls made up the majority of Do Not Call Registry complaints at the Federal Trade Commission.

As technology evolves allowing for a greater volume of robocalls, so are the tactics used to trick consumers into answering. In the past, scammers would fake caller ID information to trick consumers into thinking their bank was calling or the phone number was "unknown." Scammers are now deliberately falsifying caller ID information knowing I'm likely to answer a phone call that appears to be local, from my family, doctor or church. "Neighbor spoofing," as it's known, is a deliberate tactic behind unwanted calls and texts to both wireline and wireless phones.

Robocalls and spoofing have the potential for real financial harm. Fraud from unwanted calls amounts to almost \$9.5 billion annually, according to the FTC. It's not hard to see how scammers could use deceptive tactics to convince people – often senior citizens – to hand over their personal information or to purchase fraudulent goods and services.

Take the IRS tax scam, for example: you get an unexpected phone message claiming to be from the IRS. The call might say you owe taxes that must be paid immediately with a credit card or debit card. Scammers have been known to use the threat of a lawsuit, or arrest by the police, to convince victims to hand over bank account information.

Consumers may also get out-of-the blue calls offering to help lower debt or interest rates, or promising other "limited time" deals. Senior citizens are often targets of elderly-specific robocall scams relating to Medicare, health care, or funeral arrangements. But they are not the only ones who fall victim to these scams.

Fortunately, American consumers have options and strategies to fight robocalls and caller ID spoofing, and to protect themselves, which we will explore today with our witnesses.

The technology and tactics used by scammers may change, but as subcommittee chairman I remain focused on empowering consumers and keeping them safe from unfair, deceptive, and malicious practices.

Thank you again to our witnesses for being here today for this important discussion.